

On  
11-15-18

18 - 3144 BPG

18 - 3146 BPG

18 - 3147 BPG

**AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT, ARREST WARRANT,  
AND SEARCH WARRANTS**

I, Autumn Brown, being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. This Affidavit is submitted in support of an application for a criminal complaint and arrest warrant for Lisa Fore (“Fore”) for violations of 18 U.S.C. § 1341 (Mail Fraud) and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft) (the “TARGET OFFENSES”).
2. This Affidavit is also submitted in support of warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to search:

- a. The premises located at 4002 Shiloh Avenue, Hampstead, Maryland 21074, as further described in Attachment A-1 (the “TARGET PREMISES”);
- b. A forensic image of the hard drive of a Dell Optiplex 3020 computer, Service Tag: 9P24H52, as further described in Attachment A-2 (“TARGET DEVICE 1”),
- c. A green Lexar thumb drive, 16GB, S/N: 000-117 DB 34406-16GBA 1416S, as further described in Attachment A-2 (“TARGET DEVICE 2”)

for evidence concerning violations of the TARGET OFFENSES, as described in attachment B.

3. I am an “investigative or law enforcement officer of the United States” within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18.

FILED  
LOGGED  
ENTERED  
RECEIVED  
NOV 30 2018  
CLERK U.S. DISTRICT COURT  
DISTRICT OF MARYLAND DEPUTY  
by CEP

4. I have been a sworn law enforcement officer since 2000. I am currently a Special Agent with the Federal Bureau of Investigation and have been so employed since 2006. During my employment as an FBI Agent, I have been assigned to investigate violations of federal law including bank robbery, Hobbs Act Robbery, and offenses involving the sale and distribution of illegal narcotics. I have training and experience in the area of cellular analysis, interview and interrogation and evidence recovery.

5. The information in this Affidavit is based on my personal knowledge, training and experience, and information provided to me by other law enforcement officers and witnesses.

6. Since this Affidavit is being submitted for the limited purpose of securing a criminal complaint and search warrants, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only those facts necessary to establish probable cause to believe that the TARGET OFFENSES have been violated and that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located within the TARGET PREMISES, TARGET DEVICE 1, and TARGET DEVICE 2.

#### PROBABLE CAUSE

7. On September 13, 2018, the FBI interviewed John Cirelli concerning fraud affecting him, his father, Charles Cirelli, and certain family businesses, including the Cirelli Company, Triple C Development LP, and 7111 Chamberlain Road LLC (the "Cirelli Entities"). The corporate office of each of the Cirelli Entities is located at the Cirelli Professional Building, 537 Ritchie Highway, Severna Park, Maryland 21146.

8. For a roughly 17 year period that lasted until July 2018, John Cirelli employed Lisa Fore as a bookkeeper/assistant for the Cirelli Entities, as well as for his and Charles Cirelli's personal accounts. In connection with that role, Fore would, among other things, manage the

payment of bills and invoices and prepare checks—which were usually generated/printed from the computer at Fore’s workspace in the office (TARGET DEVICE 1)—for handwritten signature by John Cirelli or Charles Cirelli.<sup>1</sup> She was not authorized to sign checks on behalf of John Cirelli or Charles Cirelli, whether for the Cirelli Entity accounts or their personal accounts.

9. After John Cirelli would sign a check for payment to a vendor, for example, Fore would be responsible for mailing the checks to the invoicing vendor or party. Fore likewise used the Quickbooks computer program, which was installed on TARGET DEVICE 1, to assist with managing and paying bills, including by “coding” payments to various vendors. Then, after the bank statements—which reflected payments by check—would arrive to the Cirelli Entity office by mail, Fore would typically provide the statements to John Cirelli for him to review them. After he had done so, Fore was responsible for filing the statements in the office’s file room.

10. Fore was the only non-family member employee of John Cirelli and the Cirelli Entities. Her workspace, which included the TARGET DEVICE 1, was located outside of John Cirelli’s office in the Cirelli Professional Building on Ritchie Highway.

11. John Cirelli reported to the FBI that he and his family had uncovered evidence that Fore had been improperly been diverting funds from his, Charles Cirelli’s, as well as the accounts of certain of the Cirelli Entities for multiple years—beginning in 2007 (and possibly earlier) and continuing until mid-2018. Based on his and his family’s investigation, John Cirelli learned that Fore had diverted more than \$700,000 in funds for her own personal use, including by paying various credit card bills and even the property taxes associated with her residence at 4002 Shiloh Avenue, Hampstead, Maryland 21074 (the TARGET PREMISES) using the funds. Many

---

<sup>1</sup> TARGET DEVICE 1 is property of the Cirelli Entities.

of those payments were in the form of checks purporting to be signed by John Cirelli or Charles Cirelli that they did not in fact sign.

12. Fore also made unauthorized personal purchases using a company American Express card. Indeed, unauthorized credit card purchases were how the Cirelli family discovered the fraud. In late July 2018, while reviewing a statement associated with a company American Express card, Charles Cirelli's daughter discovered a roughly \$800 charge from Sam's Club and for gas that appeared to be unauthorized. She found these charges to be particularly suspicious because they were incurred around the time when Fore was on vacation in Ocean City, Maryland.

13. On August 6, 2018, John Cirelli confronted Fore concerning certain of the unauthorized American Express charges. In response, Fore said, "I did it, I'm guilty. Take it out of my paycheck." After the meeting, Fore sent a series of text messages to John Cirelli's wife regarding the fraudulent activity and expressed concern that charges would be filed. Images of the text exchanges are copied below:

Did he talk to u  
Driving with Will on way to dr appt  
2:34 PM

Should I be prepared from what he said are they going to file charges  
2:39 PM

So I can prepare my kids  
2:42 PM

I am so sorry I am sure u hate me as well thank u for being u  
2:50 PM

I don't hate you. I'm just in shock. I hope all goes well with your procedure.  
2:57 PM



I did text John didn't expect an answer  
I can't find any old receipts so is what it  
i have the one from 05 of this year I am  
cashing out my life ins policies

and that have a value  
and if I have to I will  
cash out my 401k and  
take the tax hit to repay  
I am truly sorry again

12:03 PM

14. John Cirelli terminated Fore, and he and his family continued reviewing documents, including bank statements, to determine the scope of the fraud. As noted above, this analysis revealed the diversion and theft of more than \$700,000 in funds over at least a 10 year period. All of this evidence has been provided to the FBI. John Cirelli and his family likewise discovered the existence of what appeared to be altered bank statements in the office of the Cirelli Entities. The documents consisted of bank statements that had adhered to them with scotch tape printed pieces of paper that covered and replaced information in the statement such as a description of the payee, the amount of deposits/credits, the amount of withdrawals/debits and the resulting balance. These documents were found in the office filing cabinets with other, non-altered bank statements, and were provided to the FBI. Similarly, John Cirelli provided the FBI blank bank statements—*i.e.*, statements that purported to be from a bank (and for at least one, purported to be associated with John Cirrelli's account) but that contained no listing of charges and balances—and blank Smith Mechanical invoices. Smith Mechanical was a vendor John Cirelli occasionally used. The blank Smith Mechanical invoices list no charges and enumerate no work done. These documents were located in the back of a filing cabinet secreted in Fore's employee file. These altered and blank statements and blank Smith mechanical invoices appear to have been used in connection Fore's fraud.

15. The FBI has independently obtained records associated with various credit card and bank accountants in Fore's name and that list the address of record for the accounts as the TARGET PREMISES. These records reflect unauthorized payments from certain of the Cirelli Entities, as well as John Cirelli and Charles Cirelli individually, to accounts associated with Fore.

16. For instance, a Merrick Bank account with an account number ending in 6611 reflects the following printed checks from Triple C Development, purporting to be signed by John Cirelli, and made out to Merrick Bank:

- a. Check # 3224, September 5, 2017, in the amount of \$1,926.78;
- b. Check # 3259, October 23, 2017, in the amount of \$1,589.65;
- c. Check # 3323, April 15, 2018, in the amount of \$2,478.68; and
- d. Check #3346, June 18, 2018, in the amount of \$2,179.58.

17. According to Merrick Bank records, Fore is listed as the applicant associated with the above-referenced Merrick Bank account, her husband, William Fore is listed as an authorized user, and the TARGET PREMISES is listed as the address of record. John Cirelli has reviewed copies of each of the checks referenced above and informed the FBI that the signature on it is not his and that these checks were unauthorized.

18. Likewise, a Sears credit card account (serviced by Citi) with an account number ending in 0928 reflects a July 27, 2009 check from Charles Cirelli to Sears in the amount of \$1,950.10 (Check # 3472), purporting to be signed by Charles Cirelli, and an August 25, 2009 check from John Cirelli to Sears in the amount of \$1,276.35 (Check #2026), purporting to be signed by John Cirelli.

19. According to Citi's records, Fore is listed as the applicant associated with the Sears/Citi account referenced-above, and the TARGET PREMISES is listed as the address of record.

20. John Cirelli has reviewed copies of each of the checks referenced above and informed the FBI that the signatures on the checks are forged and that the checks were unauthorized. Charles Cirelli likewise told the FBI that he did not authorize Fore to pay her personal bills, pay her taxes, or make personal purchases through the Cirelli family businesses or through his or his family member's personal accounts.

21. On October 18, 2018, the FBI obtained written to consent from John Cirelli to seize and search (1) TARGET DEVICE 1, which was used by Fore in and present in her workspace on the desk; and (2) TARGET DEVICE 2, a thumb drive also found in Fore's workspace. As noted above, TARGET DEVICE 1 is the property of the Cirelli Entities. It is unclear whether TARGET DEVICE 2 is owned by Cirelli Entities; however, as noted, it was found in Fore's workspace. I know based on my knowledge, training, and experience that it is common for places of work to have thumb drives on hand for purposes of storing and transporting documents, among other things. After receiving this consent, an FBI computer forensic IT consultant obtained an exact forensic image of TARGET DEVICE 1, so as not to have to physically remove the computer from the premises. Though John Cirelli has provided consent to search TARGET DEVICE 1 and TARGET DEVICE 2, I am nevertheless seeking warrants to search these items out of an abundance of caution.

22. As noted above, Fore used TARGET DEVICE 1 on the days that she worked, including to print checks and make authorized payments in the name of the Cirelli Entities and to run the Quickbooks application. I know based on my knowledge, training, and experience that

word processing applications on computers such as TARGET DEVICE 1 can be used to create printed text such as that taped on to the altered statements referenced above and that any documents created using such an application can be easily transported via electronic storage devices such as TARGET DEVICE 2. I also know that photocopies and scanned images of documents such as bank statements can be stored in electronic form on computers such as TARGET DEVICE 1 and electronic storage devices such as TARGET DEVICE 2. Further, based on my knowledge, training, and experience, I know that it is common for individuals involved in fraud schemes such as the one referenced above to maintain computers and electronic storage devices at their homes and to use them in connection with their scheme—for example, to facilitate the creation of fraudulent statements while at home.

23. Based on my knowledge, training, and experience, I also know that individuals who create and use fictitious or fraudulent documents such as the ones described here will often keep the documents utilized in the furtherance of their scheme in close proximity—usually at their personal residence or other private area to hide such items from law enforcement authorities.

24. Based on my training, knowledge, and experience, I further know that individuals involved in fraud schemes often maintain records, bank statements, receipts, notes, contact lists, money orders, correspondence, credit or debit cards, and other papers relating to stolen identities—such as, for example, John Cirelli—in their homes.

25. I also know that individuals involved in fraud schemes often maintain and possess documents—in electronic form or otherwise—that contain evidence of the use or possession of the personal identifying information of other individuals—including, financial and banking records, tax records, employment and payroll records, medical records and other documents in their homes.

These records are frequently maintained over an extended period, including time periods long after any particular transaction is completed.

26. Based on my knowledge, training, and experience, I know that individuals carry their cellular phones with them virtually everywhere they go and, when not outside of their homes, keep their cellular phones in near proximity in their residence.

27. On November 5, 2018, physical surveillance was conducted at the TARGET PREMISES. During that surveillance, an adult woman whose appearance was consistent with that of Fore was observed walking near the front window of the home. Further, a large "All Fore Exteriors" truck—which I understand from witnesses and my review of database records to be the name of the business owned by Fore's husband—was observed on a side street near the residence.

28. Furthermore, based on social media posts made by Fore and one of her family members I understand that Fore has booked a trip to Mexico and is scheduled to depart this weekend.

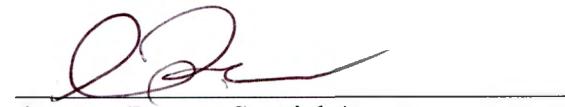
### **CONCLUSION**

29. Based on the foregoing, I respectfully submit that there is probable cause to believe that the TARGET OFFENSES have been violated and that there is probable cause to believe that evidence of these crimes can be found in the TARGET PREMISES, TARGET DEVICE 1, and TARGET DEVICE 2.

30. I thus respectfully request that the Court issue a search warrant to search the items listed in Attachments A-1 and A-2 of this Affidavit, to seize any items located pursuant to the search as described in Attachment B.

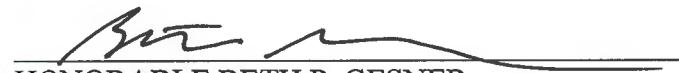
31. I further respectfully submit that there is probable cause to issue a criminal complaint and arrest warrant for Lisa Fore, charging her with mail fraud in violation of 18 U.S.C. § 1341 and Aggravated Identity Theft in violation of 18 U.S.C. § 1028A(a)(1).

32. Finally, because any search of the devices listed in Attachment A-2—which are currently in the custody of law enforcement—does not involve entry on to physical premises, reasonable cause exists to permit the execution of the requested warrants as to the devices listed in Attachment A-2 at any time in the day or night.



Autumn Brown, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this 15<sup>th</sup> day of November, 2018.



HONORABLE BETH P. GESNER  
CHIEF UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1****PREMISES TO BE SEARCHED**

The premises located at 4002 Shiloh Avenue, Hampstead, Maryland 21074. Photographs of the premises are below.



ATTACHMENT A-2

**PROPERTY TO BE SEARCHED**

The following pieces of property currently in the custody of the FBI – Annapolis, 185 Admiral Cochrane Drive, Suite 101, Annapolis, MD.

- A forensic image of the hard drive of a Dell Optiplex 3020 computer, Service Tag: 9P24H52
- A green Lexar thumb drive, 16GB, S/N: 000-117 DB 34406-16GBA 1416S,

ATTACHMENT B**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

The TARGET PREMISES, TARGET DEVICE 1, and TARGET DEVICE 2 are to be searched for all records, items, and documents set forth below, whether in paper or electronic form, relating to violations of 18 U.S.C. § 1341 (Mail Fraud) and 18 U.S.C. § 1028A (Aggravated Identity Theft):

1. All documents, records, and communications regarding (1) the Cirelli family; (2) all Cirelli family businesses, including but not limited to the Cirelli Company, Triple C Development LP, and 7111 Chamberlain Road LLC; and (3) the Cirelli Professional Building, 537 Ritchie Highway, Severna Park, Maryland 21146.
2. All documents, records, and communications regarding Fore's employment for the Cirelli family, including but not limited to her role as a bookkeeper, the payment of invoices, the writing of checks, and Fore's use of the quickbooks application.
3. All documents and records regarding the assets, finances, and tax obligations of Lisa Fore and any family member of Lisa Fore, including but not limited to financial transactions conducted by Lisa Fore and her family members; real and personal property purchased by Lisa Fore and her family members; bank accounts held by Lisa Fore and her family members; and all financial instruments or things of value associated in any way with Lisa Fore and her family members.
4. All documents relating to money, credit, and loans obtained by Lisa Fore and any Fore family and any of the entities listed herein.
5. All documents and records regarding income tax returns, records of refunds, correspondence with the Internal Revenue Service or the Comptroller of the State of Maryland or any other state, tax forms, records of online submissions, drafts, and source documentation relating to the preparation and filing of federal or state tax returns on behalf of Lisa Fore and any Fore family member.
6. All documents and records containing contact information, phone numbers, mailing addresses, email addresses, calendars, datebooks, domains, or other contact information for any of the individuals, addresses, or entities listed herein.
7. All documents and records of communications involving (i) Lisa Fore and (ii) any member of the Cirelli family.
8. Any safes, locked file cabinets, safe deposit box keys, storage locker keys, and any other access devices to locations that may contain any of the items set forth in the above-paragraphs.
9. All documents related to travel.
10. All images, messages, and communications regarding methods to avoid detection by

law enforcement.

11. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to 4002 Shiloh Avenue, Hampstead, Maryland 21074.
12. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical,

electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

13. Regarding TARGET DEVICE 1 and TARGET DEVICE 2 and any additional computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of TARGET DEVICE 1, TARGET DEVICE 2, and any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data

necessary to determine whether that data falls within the items to be seized):

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possibly recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of theft of government property or other criminal activity, the further search of that particular directory, file or storage area, shall cease.